CLAIMS

1. A method comprising:

initiating an online gaming activity from a gaming system with multiple users; and

authenticating the multiple users together in a single request/reply exchange with an authentication entity.

2. A method as recited in claim 1, wherein the authenticating comprises:

submitting a request from the gaming system to the authentication entity, the request containing identities of the multiple users; and

returning a reply from the authentication entity to the gaming system that can be used to authenticate the multiple users in the online gaming activity.

3. A method as recited in claim 1, wherein the authenticating comprises:

forming, at the gaming system, a request containing an identity string that includes a gaming system identity, multiple user identities, and an identity of an online service;

submitting the request from the gaming system to the authentication entity;

creating, at the authentication entity, a reply containing the identity string and a session key K_{XA} to be used in communication between the gaming system and the online service, the reply being encrypted with a key associated with the online service; and

returning the reply from the authentication entity to the gaming system.

4. A method as recited in claim 1, wherein the authenticating comprises exchanging messages specified in the Kerberos protocol, the response message containing a ticket having a authorization data field which acknowledges that multiple identities have been authenticated.

5. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 1.

6. A method comprising:

submitting a request from a game console to a ticket issuing entity, the request containing a game console identity, multiple user identities, and an identity of an online service;

returning a ticket from the ticket issuing entity to the game console, the ticket containing the game console identity and the multiple user identities encrypted with a key associated with the online service;

passing the ticket from the game console to the online service; and

decrypting the ticket at the online service, wherein after the decrypting the authenticity of the multiple users contained in the ticket is trusted.

7. A method as recited in claim 6, wherein the request further includes an identity of the game console, and the game console identity is included in the issued ticket.

8. A method as recited in claim 6, further comprising sending some cryptographical information to prove knowledge of the user's key while submitting the request.

9. A method as recited in claim 6, wherein the ticket further includes at least one of the online service identity, a time that the ticket is generated, a second time parameter indicative of when the ticket expires, and a randomly generated session key to be used in communication between the game console and the online service.

10. A method as recited in claim 6, wherein the returning further comprises sending an attached message along with the ticket from the ticket issuing entity to the game console, the message containing a randomly generated session key to be used in communication between the game console and the online service.

11. A method as recited in claim 10, wherein the attached session message is encrypted with a key associated with the game console.

12. A method as recited in claim 10, wherein the passing comprises sending a second message with a current time encrypted with the session key.

13. A method as recited in claim 12, wherein the ticket further includes a randomly generated session key and the verifying, at the online service, further comprises:

decrypting the ticket using the key associated with the online service to recover the session key;

decrypting the second message with the session key to recover the current time; and

authenticating the multiple users and the game console in the event that the recovered current time is within an acceptable time window from the current time.

14. A method as recited in claim 6, further comprising:

sending a reply from the online service to the game console; and

verifying, at the game console, an authenticity of the reply.

15. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 6.

16. A method comprising:

creating, at a game console, multiple validated user identities (U_1, H_1), (U_2, H_2), …, (U_U, H_U) composed of user identities U_1, U_2, …, U_U and associated values H_1, H_2, …, H_U derived from the user's key;

forming, at the game console, a request containing an identity string that includes a game console identity X, a game title identity G, the multiple validated user identities, and an identity A of an online service, as follows:

$$\text{Request} = [X, G, A, (U_1, H_1), \ldots, (U_U, H_U)];$$

submitting the request from the game console to a ticket issuing entity;

creating, at the ticket issuing entity, a ticket containing the identity string and a session key K_{XA} encrypted with a key K_A associated with the online service, as follows:

$$\text{Ticket} = E_{KA}[K_{XA}, X, G, A, U_1, U_2, U_3, U_4];$$

sending the ticket along with the session key K_{XA} from the ticket issuing entity to the game console;

passing the ticket from the game console to the online service along with data encrypted using the session key K_{XA}; and

verifying the ticket at the online service by decrypting the ticket using the online service key K_A, extracting the session key K_{XA} from the decrypted ticket, and decrypting the data from the game console using the session key K_{XA}.

17. A method as recited in claim 16, wherein the creating comprises computing cryptographic hash digests of user keys associated with the multiple users, each user identity being a combination of the user identity and the cryptographic hash of an associated user key.

18. A method as recited in claim 16, wherein the creating comprises encrypting a time value using keys associated with the multiple users, each user identity being a combination of the user identity and the current time encrypted with the user key.

19. A method as recited in claim 16, wherein the request further includes an identity of the game console.

20. A method as recited in claim 16, wherein the ticket further includes at least one of a time that the ticket is generated and a second time parameter indicative of when the ticket expires.

21. A method as recited in claim 16, further comprising encrypting the session key K_{XA} with a key associated with the game console before said sending of the session key to the game console.

22. A method as recited in claim 16, wherein the data comprises a time value representative of a current time.

23. A method as recited in claim 16, wherein the data comprises a time value representative of a current time, and the verifying comprises authenticating the game console and the multiple users in an event that the time value received from the game console is within an acceptable time window from a current time.

24. A method as recited in claim 23, further comprising:

sending a reply from the online service to the game console, the reply containing the time value encrypted using the session key K_{XA}; and

verifying, at the game console, an authenticity of the online service in an event that the game console successfully decrypts the time value using the session key K_{XA}, and the time value returned matches the time value sent to the online service.

25. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 16.

26. A method for operating a game console, comprising:

submitting a request to a ticket issuing entity, the request containing multiple user identities and an identity of an online service; and

receiving a single ticket from the ticket issuing entity that can be used to authenticate the multiple user identities to the online service.

27. A method as recited in claim 26, wherein the request further includes at least one of an identity of the game console and an identity of a game title being played in the game console.

28. A method as recited in claim 26, further comprising cryptographically deriving the user identities from information associated with the users.

29. A method as recited in claim 26, wherein the ticket includes at least one of (1) the multiple user identities, (2) the identity of the online service, (3) an identity of the game console, (4) an identity of a game title being played in the game console, (5) a time that the ticket is generated, (6) a second time parameter indicative of when the ticket expires, and (7) a randomly generated session key to be used in communication between the game console and the online service.

30. A method as recited in claim 26, further comprising sending the ticket to the online service.

31. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 26.

32. A method for operating a game console, comprising:

submitting a request to a ticket issuing entity, the request containing multiple user identities and an identity of the game console; and

receiving a single ticket from the ticket issuing entity that can be used to authenticate the multiple user identities and the game console.

33. A method for operating a game console, comprising:

creating a request with multiple user identities of multiple users who are playing on a game console; and

submitting the request to a third party.

34. A method as recited in claim 33, wherein the request includes at least one of an identity of an online service, an identity of the game console, an identity of a game title being played in the game console.

35. A method as recited in claim 33, further comprising receiving a single ticket from the ticket issuing entity that can used to authenticate the multiple user identities to another entity.

36. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 33.

37. A method comprising:

receiving a request from a game console, the request containing multiple user identities of multiple users who are playing at the game console and an identity of a third party;

generating a single ticket to be used to authenticate the multiple user identities to the third party; and

returning the ticket to the game console.

38. A method as recited in claim 37, wherein the request further includes at least one of (1) an identity of the game console and (2) an identity of a game title being played in the game console.

39. A method as recited in claim 37, wherein the ticket includes at least one of (1) the multiple user identities, (2) the identity of the third party, (3) an identity of the game console, (4) an identity of a game title being played in the game console, (5) a time that the ticket is generated, (6) a second time parameter indicative of when the ticket expires, and (7) a randomly generated session key to be used in communication between the game console and the third party.

40. A method as recited in claim 37, further comprising encrypting the ticket with a key associated with the third party prior to said returning the ticket.

41. A method as recited in claim 37, further comprising:

generating a session key to be used in communication between the game console and the third party; and

sending the session key to the game console.

42. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 37.

43. A method comprising:

receiving a request from a game console, the request containing multiple user identities of multiple users who are playing at the game console; and

issuing a single ticket to be used to authenticate the multiple user identities.

44. A method comprising:

receiving a request from a game console, the request containing multiple user identities of multiple users who are playing at the game console and an identity of the game console; and

issuing a single ticket to be used to authenticate the multiple user identities and the game console.

45. A method for manufacturing a game console, comprising:

constructing a game console with associated authentication information; and

storing the authentication information in a database to be used for authenticating the game console after the game console is released from manufacturing.

46. A method as recited in claim 45, wherein the authentication information comprises at least one of a hard disk drive ID, a CPU ID, a first value derived from the hard disk ID, a second value derived from the CPU ID, and a third value derived from a combination of the hard disk drive ID and the CPU ID.

47. A method as recited in claim 45, wherein the authentication information comprises one or more serial numbers of hardware components in the game console.

48. A method as recited in claim 45, wherein the authentication information comprises a random key generated at manufacturing time.

49. A method as recited in claim 45, further comprising securely transferring the database to an authentication site for access by an authentication server.

50. A method as recited in claim 45, further comprising creating, at the authentication server, account names/passwords for the game consoles identified in the database.

51. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 45.

52. A method for validating an authenticity of a game console, comprising:

receiving, from the game console, authentication information that is associated with the game console at a time of manufacturing; and

evaluating the authentication information to determine whether the game console is valid.

53. A method as recited in claim 52, wherein the authentication information comprises at least one of a hard disk drive ID, a CPU ID, a first value derived from the hard disk ID, a second value derived from the CPU ID, and a third value derived from a combination of the hard disk drive ID and the CPU ID.

54. A method as recited in claim 52, wherein the evaluating comprises using a database of authentication information for game consoles to determine whether the authentication is valid.

55. A method as recited in claim 52, wherein the evaluating comprises ascertaining whether an account for the game console associated with the authentication information has already been established.

56. A method as recited in claim 52, further comprising, in an event that the game console is valid, generating an identity and a cryptographic key for the game console.

57. A method as recited in claim 52, further comprising, in an event that the game console is valid, creating an account for the game console.

58. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 52.

59. A computer-readable medium for a game console comprising computer-executable instructions that, when executed, direct the game console to:

create multiple validated user identities (U_1, H_1), (U_2, H_2), …, (U_U, H_U) composed of the multiple user identities U_1, U_2, …, U_U and associated values H_1, H_2, …, H_U derived from the user's key;

form a request containing a game console identity X, a game title identity G, the multiple user identities, and an identity A of an online service, as follows:

$$\text{Request} = [X, G, A, (U_1, H_1), \ldots, (U_U, H_U)]; \text{ and}$$

submit the request to a ticket issuing entity over a network.

60. A computer-readable medium as recited in claim 59, further comprising computer-executable instructions that, when executed, direct the game console to compute cryptographic hash digests of user keys associated with the multiple users, each user identity being a combination of the user identity and the cryptographic hash of an associated user key.

61. A computer-readable medium as recited in claim 59, further comprising computer-executable instructions that, when executed, direct the game console to encrypt a time value using keys associated with the multiple users, each user identity being a combination of the user identity and the encrypted time value.

62. A computer-readable medium as recited in claim 59, further comprising computer-executable instructions that, when executed, direct the game console to form the request to further include at least one of an identity of the game console, a random nonce, and a checksum value to ensure receipt of all contents of the request.

63. A computer-readable medium as recited in claim 59, further comprising computer-executable instructions that, when executed, direct the game console to:

receive a ticket from the ticket issuing entity, the ticket containing the game console identity X, the game title identity G, the multiple user identities, the online service identity A, and a session key K_{XA} together encrypted with a key K_A associated with the online service, as follows:

$$TicketA = E_{KA}[K_{XA}, X, G, A, U_1, U_2, \ldots U_U];$$

receive the session key K_{XA} from the ticket issuing entity; and

pass the ticket from the game console to the online service along with some information encrypted using the session key K_{XA}.

64. A computer-readable medium comprising computer-executable instructions that, when executed, perform operations comprising:

receive a request from a game console, the ticket containing an identity string that includes a game console identity X, a game title identity G, multiple

user identities (U_1, H_1), …, (U_U, H_U), and an identity A of an online service, as follows:

$$\text{Request} = [X, G, A, (U_1, H_1), \ldots, (U_U, H_U)]; \text{ and}$$

generate a ticket containing the identity string and a session key K_{XA} together encrypted with a key K_A associated with the online service, as follows:

$$\text{TicketA} = E_{KA}[K_{XA}, X, G, A, U_1, U_2, \ldots U_U]; \text{ and}$$

return the ticket to the game console.

65. A computer-readable medium as recited in claim 64, further comprising computer-executable instructions that, when executed, direct the game console to generate the request to further include at least one of a time that the ticket is generated and a time length before expiration of the ticket.

66. A computer-readable medium as recited in claim 64, further comprising computer-executable instructions that, when executed, direct the game console to encrypt the session key K_{XA} with a key associated with the game console and send the encrypted session key to the game console.

67. A single gaming ticket data structure embodied on a computer readable, comprising multiple user identities of users playing at a game console, encrypted using a key associated with a third party entity to which the multiple users are to be authenticated.

68. A single gaming ticket data structure embodied on a computer readable, comprising multiple user identities of users playing at a game console and an identity of the game console, encrypted using a key associated with a third party entity to which the multiple users are to be authenticated.

69. A game console, comprising:

a memory; and

a processor coupled to the memory, the processor being configured to obtain authentication of multiple users of the game console together in a single request/reply exchange with an authentication entity.

70. A game console as recited in claim 69, wherein the request contains a game console identity, a game title identity of a game being played in the game console, multiple user identities, and an identity of an online service.

71. A game console as recited in claim 70, wherein the memory comprises a hard disk drive with an associated hard disk ID and the processor has an associated processor ID, and the processor is configured to submit at least one of the hard disk ID, the CPU ID, and a value derived from the CPU ID to a third party as part of a process to obtain the game console identity.

72. A system, comprising:

a ticketing issuing entity;

a game console configured to submit a request to the ticket issuing entity, the request containing multiple user identities and an identity of an online service; and

the ticket issuing entity being configured to generate a single ticket that can be used by the game console to authenticate the multiple user identities to the online service.

73. A system, comprising:

a ticketing issuing entity;

a game console configured to submit a request to the ticket issuing entity, the request containing multiple user identities; and

the ticket issuing entity being configured to generate a single ticket that can be used by the game console to authenticate the multiple user identities to a third party.

74. A system, comprising:

a ticketing issuing entity;

a game console configured to submit a request to the ticket issuing entity, the request containing multiple user identities and an identity of the game console; and

the ticket issuing entity being configured to generate a single ticket that can be used by the game console to authenticate the multiple user identities and the game console to a third party.